MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO PARANÁ
CONSELHO DE PLANEJAMENTO E ADMINISTRAÇÃO

RESOLUÇÃO Nº 38/22-COPLAD

Estabelece a Política de Segurança da Informação e Comunicação na Universidade Federal do Paraná.

O **CONSELHO DE PLANEJAMENTO E ADMINISTRAÇÃO (COPLAD)**, órgão normativo, consultivo e deliberativo da Administração Superior da Universidade Federal do Paraná (UFPR), em 14 de dezembro de 2022, no uso de suas atribuições conferidas pelo Artigo 18 do Estatuto da UFPR, com base no Parecer do Conselheiro Sérgio Said Staut Júnior (doc. SEI 5159460) no processo nº 036457/2021-17 aprovado por unanimidade de votos e considerando:

- o Decreto nº 9.637/2018, que institui a Política Nacional de Segurança da Informação (PNSI);

- os Arts. 24(2) e 39(1)(b), da **General Data Protection Regulation** (GDPR) e os Arts. 46 e 50 da Lei Geral de Proteção de Dados (LGPD), que primam pelas boas práticas de segurança da informação e privacidade;

- a Portaria nº 93/2019 do Gabinete de Segurança Institucional da Presidência da República, que aprova o Glossário de Segurança da Informação;

- a Instrução Normativa (IN) nº 01/2020 do Gabinete de Segurança Institucional/Presidência da República, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal; e

- a Portaria nº 395/2021/UFPR, que cria o Comitê Institucional de Governança Digital e Subcomitês.

RESOLVE:

Art. 1º Aprovar a Nova Política de Segurança da Informação e Comunicação (POSIC).

CAPÍTULO I
DO OBJETIVO, TERMOS E DEFINIÇÕES

Art. 2° A Política de Segurança da Informação e Comunicação da Universidade Federal do Paraná observará os princípios, objetivos e diretrizes estabelecidos nesta Resolução, bem como as disposições constitucionais, legais e regimentais vigentes.

Parágrafo único. Integram, também, a POSIC outras normas e políticas específicas de segurança da informação e comunicação, bem como as que tratem de privacidade, acesso à informação, utilização de recursos de Tecnologia da Informação e Comunicação (TIC), dentre outras.

Art. 3º A POSIC estabelece as orientações e diretrizes corporativas gerais de segurança e controle dos ativos de informação da UFPR ou sob sua guarda, objetivando sua proteção e a prevenção de responsabilidade legal para todos os usuários.

Art. 4º As medidas de segurança da informação e comunicação devem ser planejadas, aplicadas, implementadas e, periodicamente, avaliadas de acordo com os objetivos institucionais e os riscos para as atividades da Universidade.

Art. 5º Para efeitos desta Resolução, considerar-se-á prioritariamente as definições do Glossário de Segurança da Informação (Portaria nº 93/2019 do Gabinete de Segurança Institucional da Presidência da República) e, complementarmente, as definições a seguir:

I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

II - ativo da informação: os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios e também os recursos humanos que a eles têm acesso;

III - documento: unidade de registro de informações, qualquer que seja o suporte ou formato;

IV - dado pessoal: qualquer informação relacionada a pessoa natural identificada ou identificável;

V - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

VI - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VII - tratamento de dados: toda operação realizada com dados de quaisquer naturezas, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

VIII - segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

IX - gestor da informação: responsável por unidade da Universidade que, no exercício de suas competências, produz informações ou obtém, de fonte externa à Universidade, informações de propriedade de pessoa física ou jurídica;

X - gestor da segurança da informação: pessoa formalmente indicada por ato da Reitoria para atuar como responsável pela gestão da segurança de informação e comunicação na Universidade, nos termos da PNSI;

XI - custódia: consiste na responsabilidade de se guardar um ativo de informação para terceiros. A custódia não permite automaticamente o acesso ao ativo e nem o direito de conceder acesso a outros;

XII - custodiante: aquele que, de alguma forma, total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema de informação - ou dos ativos de informação que o compõem - que não lhe pertence, mas que está sob sua custódia, como por exemplo, a Agência de Tecnologia da Informação e Comunicação (AGTIC) ou provedores externos de serviços de TIC, que armazenam sistemas, bancos de dados, repositórios de arquivos, domínios, sítios eletrônicos, entre outros;

XIII - custodiante da informação: qualquer indivíduo ou unidade da UFPR que tenha por atribuição, ou não, o acesso a ativos de informação em determinado momento, mesmo que transitório, e que tem a responsabilidade de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação comunicadas pelo proprietário da informação;

XIV- colaborador: servidores docentes ou técnico-administrativos, terceirizados, parceiros e outras partes envolvidas com a UFPR que lidem com a informação produzida ou recebida pela universidade;

XV - incidente de segurança da informação: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação, das redes de computadores, bem como em outros ativos de informação;

XVI - **General Data Protection Regulation** (GDPR): lei europeia que objetiva a proteção de dados pessoais de seus cidadãos e aplica-se a qualquer entidade que faça uso de dados de cidadãos europeus;

XVII - Lei Geral de Proteção de Dados (LGPD): é a lei que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

a) a operação de tratamento seja realizada no território nacional;

b) a atividade de tratamento que tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou

c) os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

XVIII - encarregado de proteção de dados pessoais: pessoa indicada pela Reitoria para atuar como canal de comunicação entre a Universidade, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD);

XIX - Autoridade Nacional de Proteção de Dados: agência reguladora brasileira da Lei Geral de Proteção de Dados Pessoais; e

XX - usuário: pessoa física ou natural, internas ou externas à Universidade, habilitada pela administração para acessar seus ativos de informação.

CAPÍTULO II
DA ABRANGÊNCIA

Art. 6º Esta política aplica-se a todos os usuários, devendo ser lida e conhecida por todos os usuários da informação.

Art. 7º A POSIC é aplicável ao ambiente digital ou físico de armazenamento da informação. Abrange todos os equipamentos e sistemas possuídos ou utilizados pela Universidade para estes fins.

Art. 8º Cabe ao usuário de informações a observância das regras e fica vedado alegar desconhecimento da POSIC.

§ 1º Esta política deve ser comunicada para todo o pessoal envolvido e largamente divulgada, garantindo que todos a conheçam e a pratiquem.

§ 2º A inobservância das políticas e normas de segurança sujeita o usuário a sanções internas e, nos casos cabíveis, às leis vigentes.

CAPÍTULO III
DOS ATRIBUTOS E PRINCÍPIOS

Art. 9º A segurança da informação e comunicação, coberta pela presente POSIC, terá, dentre outros inerentes à Administração Pública Federal, os seguintes atributos:

I - confidencialidade: propriedade de que a informação estará disponível e somente será revelada a pessoa física, sistema, órgão ou entidade que esteja autorizada e credenciada;

II - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

III - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental; e

IV - autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

Art. 10. A POSIC terá, dentre outros inerentes à Administração Pública Federal, os seguintes princípios:

I - responsabilidade: preservação da integridade e tratamento de maneira adequada da informação, de acordo com sua classificação, bem como preservar e zelar pelos ativos de informação;

II - clareza: as regras que se fundamentam na POSIC devem ser claras, objetivas e concisas, a fim de viabilizar sua fácil compreensão; e

III - publicidade: transparência às informações públicas, como preceito geral, respeitando a privacidade do titular, nos termos da LGPD.

CAPÍTULO IV
DO ACESSO À INFORMAÇÃO

Art. 11. A Universidade priorizará e promoverá a divulgação de informações de interesse público, independentemente de solicitações, fazendo uso de meios de comunicação viabilizados pela tecnologia da informação para facilitar o acesso.

Art. 12. O acesso às informações produzidas ou custodiadas pela Universidade, que não sejam de domínio público, deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades de seus colaboradores.

§ 1º Qualquer outra forma de uso que extrapole as atribuições necessárias ao desempenho das atividades dos usuários internos, discentes ou colaboradores necessitará de prévia autorização formal, pelo custodiante.

§ 2º O acesso, quando autorizado, dos usuários discentes, colaboradores ou externos a informações produzidas ou custodiadas pela Universidade que não sejam de domínio público é condicionado ao aceite a termo de sigilo e responsabilidade.

Art. 13. Qualquer interessado poderá apresentar pedido de acesso a informações aos órgãos e unidades desta Universidade, por qualquer meio legítimo, devendo o pedido conter a identificação do requerente e a especificação da informação requerida, conforme preconizado pela Lei de Acesso à Informação.

§ 1° Para o acesso a informações de interesse público, a identificação do requerente não pode conter exigências que inviabilizem a solicitação.

§ 2° A Universidade priorizará que os pedidos de informação sejam solicitados ao Serviço de Informação ao Cidadão (SIC), que classificará e encaminhará à unidade correspondente.

§ 3° Esta Resolução não disciplina e não se aplica a pedidos de informações relacionados aos Processos Seletivos, Concursos Públicos, Processos Avaliativos e demais processos classificatórios, que pela natureza da concorrência, serão regidos por editais próprios.

CAPÍTULO V
DA SEGURANÇA, PROTEÇÃO DE DADOS E PRIVACIDADE

Art. 14. A Universidade fará uso de tecnologias e boas práticas na gestão da informação para garantir a segurança, proteção e privacidade de seus dados em conformidade com esta política e com as demais normas complementares, bem como a correta implementação das seguintes diretrizes:

I - tratamento de dados;

II - segurança física e do ambiente;

III - gestão de incidentes em segurança da informação;

IV - gestão de ativos de TIC;

V - gestão do uso dos recursos operacionais e de comunicações, como: e-mail, acesso à internet, mídias sociais, computação em nuvem, dentre outros;

VI - controles de acesso;

VII - gestão de riscos;

VIII - gestão de continuidade; e

IX - auditoria e conformidade.

CAPÍTULO VI
DOS DEVERES E RESPONSABILIDADES

Art. 15. Compete ao Comitê Institucional de Governança Digital (CIGD) ou instância equivalente, zelar pela implementação e manutenção da POSIC, nos termos do regulamento vigente.

Parágrafo único. Esta Resolução observará as competências do Comitê Institucional de Governança Digital, do Subcomitê de Estratégias e Soluções de TIC (SETIC) e do Subcomitê de Segurança da Informação e Privacidade (SSIP), criados em portaria da Reitoria.

Art. 16. Compete aos pró-reitores, dirigentes e chefias imediatas:

I - conscientizar usuários internos e colaboradores sob sua supervisão em relação aos conceitos e às práticas de segurança da informação e comunicação;

II - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à segurança da informação e comunicação;

III - tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação e comunicação por parte dos usuários internos ou externos e colaboradores sob sua supervisão;

IV - garantir a proteção de dados pessoais sob sua custódia, nos termos da LGPD, recorrendo ao encarregado de proteção de dados pessoais, quando necessário; e

V - informar ao gestor da informação caso sejam encontradas inconsistências em registros que cheguem ao seu conhecimento.

Art. 17. Compete aos Gestores da Informação:

I - adotar as medidas e procedimentos necessários para garantir a segurança e a privacidade das informações;

II - definir procedimentos, critérios de acesso e classificar as informações, observados os dispositivos legais e regimentais relativos ao sigilo e a outros requisitos de classificação pertinentes; e

III - propor regras específicas ao uso das informações.

§ 1º As informações recebidas de pessoa física ou jurídica externa à Universidade serão submetidas, adicionalmente, a medidas de segurança da informação, compatíveis com os requisitos pactuados com quem as forneceu.

§ 2º Os servidores em função de chefia podem indicar, orientar e autorizar, a qualquer tempo, procedimentos que visem garantir a segurança da informação, nos processos e documentos de sua competência, a serem seguidos pelos gestores da informação pertinentes.

§ 3º Compete aos colaboradores da UFPR informar imediatamente ao Gestor da Informação ou sua chefia imediata, quando encontrarem inconsistências em registros, para que este tome as medidas cabíveis.

Art. 18. Compete ao custodiante e ao custodiante da informação:

I - garantir a segurança da informação sob sua posse, conforme os critérios definidos pelo proprietário dos dados;

II - comunicar tempestivamente ao gestor da informação e/ou proprietário dos dados sobre situações que comprometam a segurança das informações sob custódia;

III - comunicar ao gestor e ou proprietário da informação eventuais limitações para cumprimento dos critérios definidos pelo Gestor de Segurança da Informação; e

IV - encaminhar demandas de fornecimento de dados e informações custodiadas ao gestor e ou proprietário das informações para que este(s) decida(m) acerca da cessão.

Art. 19. Compete ao Gestor da Segurança de Informação:

I - promover a cultura de segurança na Universidade;

II - acompanhar as investigações e avaliações dos danos decorrentes de quebra de segurança na Universidade;

III - atuar em conjunto com os Gestores de Informação na investigação e tratamento de incidentes de segurança da informação e comunicação na Universidade; e

IV - propor recursos necessários às ações de segurança da informação e comunicação na Universidade.

Art. 20. Compete ao Encarregado de Proteção de Dados Pessoais, em relação à privacidade:

I - aceitar reclamações e comunicações dos titulares de dados mantidos na UFPR, prestar esclarecimentos e adotar providências;

II - receber comunicações da ANPD e adotar providências; e

III - orientar os colaboradores a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

Art. 21. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pela Universidade devem observar, no que couber, os dispositivos integrantes da POSIC.

CAPÍTULO VII
DAS DISPOSIÇÕES FINAIS

Art. 22. A não observância dos dispositivos da POSIC pode acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 23. A periodicidade para a revisão da Política de Segurança da Informação não deve exceder 4 (quatro) anos.

Art. 24. Os casos omissos nesta Resolução serão decididos pelo CIGD, ou órgão equivalente, em primeira instância e ao COPLAD em segunda instância.

Art. 25. Revogar a Resolução nº 21/14-COPLAD.

Art. 26. Esta Resolução entra em vigor na data de sua publicação.

Ricardo Marcelo Fonseca
Presidente

Documento assinado eletronicamente por **RICARDO MARCELO FONSECA**, **REITOR**, em 20/12/2022, às 16:08, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida aqui informando o código verificador **5179772** e o código CRC **6A524F2E**.

Referência: Processo nº 23075.036457/2021-17 SEI nº 5179772